TNC-UTM: A Holistic Solution to Secure Enterprise Networks

Fachao Deng[1,2], Anan Luo[3], Yaokun Zhang[3], Zhen Chen[1,4], Xuehai Peng[3],Xin Jiang[3], Dongsheng Peng[3]
[1]*Research Institute of Information Technology, Tsinghua University, Beijing, China*
[2]*Department of Automation, Tsinghua University, Beijing, China*
[3]*Department of Computer Science and Technology, Tsinghua University, Beijing, China*
[4]*Tsinghua National Lab for Information Science and Technology, Beijing, China*
dfc03@mails.tsinghua.edu.cn

Abstract

This paper presents TNC-UTM, a holistic solution to secure enterprise networks from gateway to endpoints. Just as its name suggested, the TNC-UTM solution combines two popular techniques TNC and UTM together by defining an interface between them that integrates their security capacity to provide efficiently network access control and security protection for enterprise network. Not only TNC-UTM provides the features of TNC and UTM, but also it achieves stronger security and higher performance by introducing intelligent configuration decisions and RBAC mechanism. Experiment demonstrated the superior advantages of the TNC-UTM solution.

Keywords: TNC, UTM, holistic, access control

1. Introduction

With fast development of the Internet, network security becomes an important issue, as large numbers of security threats exist in current Internet, such as virus, worms, trojans and malicious attacks. It is even worse for enterprise networks, where loss of key data and network breakdown can usually cause tremendous damage for businesses and companies.

There has already been some network connect and access control mechanisms, such as 802.1x, VPN, and firewall, as well as some protection technologies, which includes intrusion detection system (IDS), anti-virus, anti-spam. However, security breaches are still causing significant losses and damages. An endpoint security survey of 2007 [1] states that, there was still a high percentage of malware infection: 43.3% of companies surveyed were hit by computer viruses in the last past 12 months and 18% hit by spyware.

There are mainly two reasons for the security problems. One is that diversity of various security products that restricts the efficiency of security defense systems; the other is because of endpoint mobility and the lack of endpoint security protection mechanisms, which makes it easier for worms and virus to infect network through endpoint hosts.

In order to design essential effective protection for the enterprise networks with a focus on the two problems mentioned above, three design principles for the design of a holistic security solution are present:

The capability of gateway devices should be more and more powerful under the condition of performance guarantee. It would be better for one device to cover all the protection functions, which can reduce management cost and complication. Being a typical all-in-one device, Unified Threat Management (UTM) [8] is gaining popularity for boundary gateway. Unfortunately, most of current UTM products cannot provide performance guarantee [2].

All the users and hosts that access/connect to network should be properly authenticated and authorized with the right security policies. Not only authentication and authorization of users, but also authentication and assessment of endpoint hosts are needed. Trusted Network Connect (TNC) [3] can satisfy this requirement, which provides a set of mechanisms for protecting endpoint access security while ensuring information integrity of endpoints.

The overall objective of gateways and endpoint hosts should enforce the access control for sensitive and confidential data. Generally each company has its own data servers to store a mass of proprietary information, and all the access to the sensitive data servers must be controlled and monitored. Several access control models, such as Role based access control (RBAC) model [4] and Task based authorization control model (TBAC) [5], have been proposed. RBAC model is used widely. However, independent TNC architecture or UTM devices cannot fully achieve complete access control to servers.

The TNC-UTM solution proposed in this paper, which is designed following the three principles, is a holistic solution to secure enterprise networks. It not

only provides features of TNC and UTM, but also achieves the following two advantages:

First, the protection capabilities of endpoint and gateway are coordinated, which makes TNC more flexible when enforcing policies, and saves the computing and communicating resources of UTM. Second, RBAC mechanism can be enforced to restrict the unauthorized access to sensitive server network.

The rest of this paper is organized as follows: Section 2 gives a brief description of the research background. Section 3 presents overview of our solution TNC-UTM, and design details are followed in section 4. Some experimental results are illustrated and analyzed in section 5, and finally we give our conclusion and future works in section 6.

2. Background

2.1. Trusted Network Connect

TNC is an open standard network access control architecture, which is defined and promoted by Trusted Computing Group (TCG). The definition of TNC is "enables network operators to enforce policies regarding the security state of endpoints in order to determine whether to grant access to a requested network infrastructure" [3].

The architecture of TNC is composed of five entities: Access Requestor (AR), Policy Decision Point (PDP), Policy Enforcement Point (PEP), Metadata Access Point (MAP), and Flow Controllers and Sensors. The two entities AR and PDP are required by TNC architecture, while the other three are optional.

The TNC authorization process can be summarized in five stages. (1) AR collects health status information of the endpoint, which may include information about the software of OS, anti-virus, firewall and so on. (2) Then AR sends the information about state of health and user identity to PDP. (3) PDP authenticates user's identity and evaluates health status of AR with certain security policies, and then makes decision whether AR can be grant access the network. (4) After that, PDP sends the decision to PEP which executes the decision made for the corresponding AR. (5) PEP enforces policies and controls access to the protected network.

With the help of Trusted Platform Module (TPM) [6] and interface IF-PTS [7], TNC can assure the information that AR reports are trusted.

2.2. Unified Threat Management

Unified Threat Management [8] security appliance products include multiple security features integrated into one device. The appliance must be designed and implemented functionally of network-based firewall, network-based intrusion detection and prevention, and gateway anti-virus. All of these functions must be integrated inherently into the appliance even when some may not be utilized fully.

As a security gateway, UTM usually locates at network access points. The enterprise network contains two main parts, client network for employee, and server network which contains company's sensitive data. There are mainly two tasks for UTM:

Internal network protection: By taking advantage of its ability of firewalling, intrusion detection and anti-virus, the network flows between Internet and Enterprise Network are filtered and monitored.

Server network protection: In order to protect critical resources, UTM should forbid any access to server network outside and restrict access from internal users by setting up corresponding firewall policies.

2.3 Limitations of UTM

However, current UTM products cannot achieve two tasks mentioned above very well, and the reasons are present as follows:

First, UTM provides several protect mechanisms for internal network protection without performance guarantee, sometimes even very slow especially when enabling Anti-virus or IDS functions. The problem occurs because handling data or flows in application layer results in more system costs, as gateway devices working on network layer.

Some classical algorithms of pattern matching are introduced in literature [9], but using pattern matching algorithm in UTM, performance cannot be improved significantly. Most of the hosts in internal network have installed anti-virus software and host-based IDS to protect themselves. It seems wasting UTM's capability to filter the flows to those hosts with high protection capabilities. Thus, it will enhance performance significantly if UTM only filters the flows to hosts with low self protection capabilities.

Using TNC, we can easily evaluate protection capabilities of endpoint hosts. In our design, we consider UTM as a PEP entity of the TNC architecture, and design interaction interface between them to implement UTM protection mechanisms based on endpoint self protection capabilities to avoid redundant security checks and thus gain better processing speed.

For the aspect of server network protection, we would like to deploy some specific high-level policies for accessing sensitive data from authorized users, e.g. "Employees in finance department can access finance server". However, as a gateway device, UTM can only catch the packets from specific IP address, which can be easily spoofed, so UTM cannot figure out user

identity of packets. In order to deploy the high-level policies, we need to bind packets' IP addresses with user identities reliably and securely. By taking advantage of TNC, we can achieve this much easily.

3. Overview of TNC-UTM

Figure 1 shows a typical TNC-UTM deployment. The host, 802.1x enabled switch, PDP, and remediation server are typical TNC components. When the host connects via an 802.1x enabled switch or access point (AP) to the enterprise network, the TNC client installed in the host measures health status of the host and reports it to the PDP. It also reports the IP address of the host, right after the host gets an IP address (by static configuration or DHCP).

We now consider the following four activities that define how TNC-UTM works.

Registration.

Network policies, including information of all registered users, should be built at the PDP when set up, so that users can be authenticated when accessing the network. As a simple case, users may be authenticated by their user name and password.

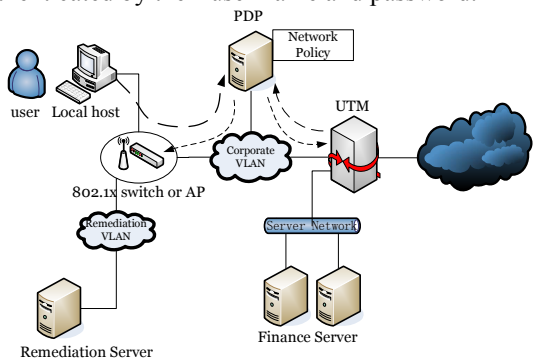

Figure 1. An example of TNC-UTM deployment.

Authentication and Assessment.

1. A user connects to the network from a host. TNC client measures the health status of the host, and sends the information to PDP through an 802.1x enabled switch or AP which has its ports "half-closed" before the authentication and assessment successfully completed.
2. PDP checks user's identity and assesses host's health status. After that, PDP knows the user's role and host protection capabilities, and then makes access and protection decisions. PDP notifies switch whether the port connected by the host should be opened and which VLAN the host should belong to.
3. When the host acquires an IP address, the TNC client reports it to PDP, and PDP binds the IP address, user, MAC address, roles, protection capabilities, and switch information together. PDP notifies UTM what resources in the server network the IP address can access through the UTM according to the user's corresponding roles, and what protection actions should be adopted according to the host's corresponding protection capabilities.

Enforcement.

1. The switch follows PDP's decision, and takes actions to allow, disallow or isolate the host.
2. The UTM receives PDP's instruction, and adds an entry to its UTM-IP-Auth table, associating host IP address with roles, protection actions, and timeout value. Based on IP and roles, UTM creates dynamic firewall policies to enforce access control to resources in the server network.

Flow Setup.

On receipt of a packet, UTM firewall will filter the packet with dynamic firewall policies and static firewall policies [10]. Resource access control enforced here is some kind of RBAC mechanism, because it is based on users' roles that the dynamic firewall policies are set up by UTM.

Because of the sensitivity of server network, all flows between client network and server network should be taken full protection actions, which means all flows between client network and server network, are scanned by anti-virus engine and IDS engine.

If IDS engine detects any abnormal flow from the client network, UTM will report the client IP and event to PDP, and PDP will make a new decision to deal with this client host. For example PDP may instruct the 802.1x enabled switch or AP to close the port that the host connects to.

If the packet's destination is the Internet, and is allowed by firewall engine, UTM will take protection actions to the data flow, which the packet belongs to, according to the entry of UTM-IP-Auth table matched by the flow. The protection actions here may be only anti-virus, only IDS, anti-virus and IDS or neither but forward directly. Generally, the UTM only enforce the security check to the data sent from the Internet to internal network.

4. Design of TNC-UTM

4.1. UTM

In order to improve performance of UTM, we propose UTM should give different protections to different hosts according to the different protection capabilities of the hosts. In order to use RBAC mechanism, we propose UTM should set up dynamic firewall policy. These two aspects are not commonly

considered in current UTM products, so we need to add a new part of design to UTM. In our solution, four tables should be added into UTM, some of which have been mentioned in section 3.

UTM-IP-Auth table. The UTM-IP-Auth table contains four fields: *source IP address*, *roles*, *protection number*, and *timeout value*. It describes that all the packets from this *source IP address* are sent by a user who has these *roles*, and UTM should give this *source IP address* protections indicated by the *protection number*. The permissions associated to the roles will be explained in UTM-Role-Resource table, and the meaning of protection number will be explained in UTM-Protection-Action table.

Only the PDP can add entries to the UTM-IP-Auth table. Entries will be removed when timeout due to inactivity or by the PDP. The PDP might remove an entry belonging to a host when it does not qualify for network access, or it has just left the network.

UTM-Role-Resource table. The UTM-Role-Resource table contains two fields: *role* and *resources*. It describes the association between roles and resources authorized. We recommend expressing resources in URL (RFC1738) format:

protocol://IPaddress:port.

For example, tcp://192.168.1.10:80. UTM-Role-Resource table and UTM-IP-Auth table have a common field *role*. Considering them together, UTM knows which source IP address could access what resources, and then generates dynamic firewall policies.

UTM-Role-Resource table is firstly generated and stored in PDP by network policies. When a connection between UTM and PDP is just set up, the PDP pushes the table to UTM. And only PDP can update the table.

UTM-Protection-Action table. The UTM-Protection-Action table is a mapping table between *protection number* and *protection actions*. For example protection number 1 means UTM does not enable anti-virus engine but IDS engine. (See section 4.2.) Like UTM-Role-Resource table, the UTM-Protection-Action table is also pushed to UTM by PDP when a connection between UTM and PDP is just set up.

Dynamic firewall policies table. The dynamic firewall policy contains six fields: *source IP address, destination IP address, destination port, protocol, protection number, timeout value*. This table is generated by UTM considering both UTM-IP-Auth table and UTM-Role-Resource table, and updated when any of the two tables changes. However, the protection number here, which indicates the protection actions between client network and server network, is not equal to the protection number in UTM-IP-Auth table, which indicates the protection actions between client network and the Internet. Generally, UTM should take full protection actions here.

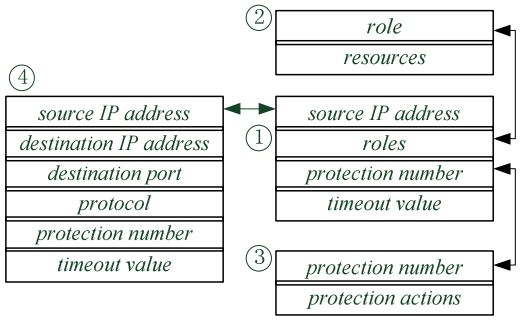

Figure 2. Relationship between tables

Figure 2 shows the relationship between the four tables: ① UTM-IP-Auth table; ② UTM-Role-Resource table; ③ UTM-Protection-Action table; ④ Dynamic firewall policies table.

4.2. Policy Decision Point

The PDP is the "brain" of the network, and network administrator deploys policies here. TNC architecture specification [3] recommends two technologies to implement PDP: RADIUS (RFC2865) and Diameter (RFC3588). No matter which technology adopted, the PDP should finish these tasks: (1) Parse the network policies, and know what resource the roles have permission to access, what protection actions the protection number indicates. (2) Authenticate user identity, and assign roles to the user. (3) Assessment host health status, get host protection capabilities and assign protection number to the host. (4) Binds the IP address, user, MAC address, roles, protection capabilities, and switch information together. (5) Send decisions to 802.1x switches and UTM.

In our solution, we record role-resource and user-role separately. Figure 3 and Figure 4 give samples of the two records. The role-resource record will be sent to UTM when the connection between PDP and UTM is just set up and UTM will generate UTM-Role-Resource table.

```
  #role      :     resources
 "CEO"       :   "tcp://192.168.1.10:80"
                   &"tcp://192.168.1.11:80"
                   &"tcp://192.168.1.12:21"
                   &"tcp://192.168.1.13:8080";
"manager"    :   "tcp://192.168.1.12:21";
"accountant":   "tcp://192.168.1.13:8080";
"employee"  :   "tcp://192.168.1.10:80"
```

Figure 3. A sample Role-Resource record

```
#user name :     roles
   "Alice"  : "accountant"&"employee"
   "Bob"    : "accountant"&"manager"
   "Frank"  : "CEO"
```

Figure 4. A sample User-Role record

We recommend that assessment policy should consist of a condition and corresponding decisions. The condition is host status, which contains OS patch, anti-virus software, IDS software, and firewall software operating situation. Anti-virus and IDS software operating situation stands for the protection capabilities of the host. Decisions are divided into two types: decisions to 802.1x switch and decisions to UTM. Decisions to 802.1x switch are usually be "allow or deny to some VLAN", and decisions to UTM are generally protection actions. Table 2 shows a sample assessment policy, and VLAN0 and VLAN1 indicates the remediation VLAN and corporate VLAN separately. We use a protection number to stand for a group of protection actions. See Table 1. And this table will be sent to UTM when the connection between PDP and UTM is just set up.

Table 1. Protection-Action table

Protection number	Protection actions	
	Anti-virus	IDS
0	Disable	Disable
1	Disable	Enable
2	Enable	Disable
3	Enable	Enable

Table 2. A sample assessment policy

Conditions				Decisions	
OS	AV	IDS	firewall	switch	UTM (Protection No.)
×	×	×	×	deny	/
×	√	√	√	VLAN 0	/
√	×	√	√	VLAN1	2
√	√	√	√	VLAN1	0

4.3. Message Flow between PDP and UTM

When PDP and UTM set up a connection, they will set up a secure SSH path assuring the messages transported between PDP and UTM are encrypted. And after that PDP will push Role-Resource records and Protection-Action table to UTM, which are generated from network policies.

On receipt of the records and table, UTM will update its UTM-Role-Resource table and UTM-Protection-Action table. When PDP makes a decision for a host who requests to access the network, PDP will send a 4-tuple data (source IP address, roles, protection number, timeout value) to UTM, which will update UTM-IP-Auth table. If PDP detects a host no longer qualifies for network access, PDP will send a command to UTM to remove the corresponding entry of UTM-IP-Auth table. When IDS engine of UTM detects an abnormal behavior from an IP address, UTM will generate an event to describe the abnormal behavior, and send the IP/event pair to PDP.

5. System Evaluation

In a word, our solution can provide effective protection to enterprise network, and improve UTM performance obviously at the same time. Furthermore we give several security considerations for some typical sceneries and performance evaluation of UTM under our solution.

5.1. Security Considerations

An attacker may fake an IP address which has the privileges to access confidential server network, and spoofs the server network as a legitimate user. In this case, the attacker must control a host, and authenticate to PDP for access enterprise network. This attack can be thwarted by TNC because PDP can detect this change by TNC client's reporting of the IP address's change. The TNC client's availability can be guaranteed by the TPM in host [7, 8].

Another possible attack is that attackers can still intrude the hosts with high protection ability because of some wrong operations made by users or wrong policies made by network administrator. Therefore, in our design, TNC-UTM still needs to filter these flows randomly and periodically instead of "all pass"; the timeout value of UTM-IP-Auth table is used to check the availability lifetime of host protection ability in order to avoid some un-predictable change of host health status.

5.2. Performance Evaluation

It is obviously that when UTM only filters the flows to hosts with low self protection capabilities in our solution, its overall processing speed could be improved. In this section, we design an experiment to show that, how much performance improvement can be achieved.

In the experiment, we use a UTM device based on an Intel 2.0GHz Pentium 4 processor, 4G RAM, and two Gigabit Ethernet NICs. This UTM device is running Linux OS and different security facilities. And we took advantage of several open source software to simulate UTM functions: Iptables is used for firewall, Snort is used for intrusion detection, and Clam-AV is used for gateway anti-virus.

The inbound traffic flows through the UTM were generated between four client-server pairs of computers, and they all passed through UTM. These

computers were HP file servers with four Intel 2.8GHz Pentium 4 processors. Four clients downloaded files as fast as they could through HTTP Get operation from four servers separately. Each file was 100KB, and we tested how many files the clients could download in 1 minute. By this means, we could calculate the processing speed of UTM.

The experiment was conducted for five times. We deployed different policies for clients with different protection capabilities. The flows to hosts with high capabilities did not need to be checked by UTM, while the flows to hosts with low capabilities needed to be checked carefully. For each time, different percent of clients had high protection capabilities, and the proportion is shown in Table 3. The results are shown in Figure 5. The horizontal axis represents different times, while the vertical axis represents overall processing speed of UTM.

Table 3. Five tests with different settings.

Times	1	2	3	4	5
percent	0	25%	50%	75%	100%

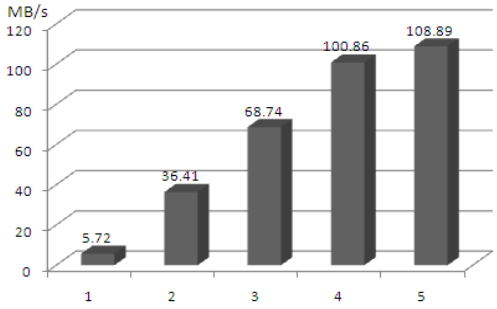

Figure 5. Processing speed of UTM

At the first time, all the flows needed to be checked by UTM, and the processing speed was only 5.72MB/s. However, when 50% clients had high protection capabilities in the third time, the processing speed improved to 68.78MB/s, 12 times of the first time. At the fifth time, the UTM had reached its maximum processing speed with the restriction of Gigabit Ethernet NIC. From the experiment, we can arrive at the conclusion that the more clients have high protection capabilities, the better performance improvement can be achieved by our solution.

6. Conclusion and Future Work

In this paper, we present a holistic solution TNC-UTM to secure enterprise networks. With TNC-UTM, we can not only ensure that the features of TNC and UTM are implemented, but also bring additional benefits by integrating TNC and UTM. The protection capabilities of endpoint and UTM are coordinated, which saves the computing and communicating resource of UTM and improves its processing speed. And also RBAC mechanism can be enforced to restrict the unauthorized access to sensitive server network.

A TNC-UTM system prototype is under development. We have implemented the TNC part of our solution based on the open source project TNC@FHH [11]. More performance analysis will appear in our future works.

Acknowledgments

This paper is supported by the National High Technology Research and Development Program of China (No. 041402003), Basic Research Development Program of China (No. 2006cb708301) and "Trusted Software" Program of Natural Science Foundation of China.

References

[1] Hong Kong Productivity Council. Endpoint Security Survey 2007. Nov. 2007;
[2] Y. Qi, B. Yang, B. Xu, and J. Li. Towards System-level Optimization for High Performance Unified Threat Management. Proc. of the 3rd International Conference on Networking and Services. 2007.
[3] Trusted Computing Group. TNC Architecture for Interoperability Specification Version 1.3. Apr. 2008.
[4] D. Ferraiolo and R. Kuhn. Role-Based Access Control. Proc. of the 15th National Computer Security Conference. 1992.
[5] R.K.Thomas and R.S.Sandhu. Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. Porc. of the IFIP WG11.3 Workshop on Database Security. 1997.
[6] Trusted Computing Group. PC Client Specific Trusted Platform Module TPM. Version 1.2. Mar. 2008.
[7] Trusted Computing Group. TCG Trusted Network Connect TNC IF-PTS. Technical report. 2006.
[8] http://www.idc.com/
[9] B.W.Watson and G.Zwaan. A Taxonomy of Keyword Pattern Matching Algorithms. Computing Science Note 92/27. Dec. 1993.
[10] D.E.Taylor. Survey & Taxonomy of Packet Classification Techniques. ACM Computing Surveys, Volume 37, Issue 3, 238-275. Sep 2005.
[11] http://tnc.inform.fh-hannover.de/wiki/index.php