

Juniper UAC demo

Filip Elsen
21 June 2010

Labo network layout



Devices used in this demo;

- Juniper IC4000
- Juniper ISG1000
- Juniper Odyssey client
- Windows Xp client
- Microsoft Windows AD/CA
- Cisco Cat3750
- Webserver
- Bluecoat proxy
- Infoblox dhcp/dns

Be aware at any time who is connected to the network and control the access that is granted to the end-user.

1. Guest vlan

Who? External users which are unknown in the domain.

- >Internet access after authentication on the guest portal.
- >Guest login credentials provided by reception.
- >No Odyssey client.
- >URL redirection on firewall

2. User authentication with machine certificate validation

->Compliant: Normal lan access

->Remediation:

- *revoke certificate / AntiVirus / notepad

- *Host enforcer policy: icmp webserver, but no http (server is in same subnet).

- *Firewall policy enforced - only internet access via proxy – policy logging.

3. Machine Authentication

->Compliant: Normal lan access

->Remediation:

*Host enforcer policy: icmp webservice, but no http (server is in same subnet).

*Firewall policy enforced - only internet access via proxy – policy logging.

4. Critical vlan

What? In case of emergencies, when the connectivity is broken between the switch and the Infranet Controller.

->New authentication requests will be set in the remediation vlan without authentication.

->When the radius becomes available again: re-initiate 802.1x.



Q&A
