



Interested in learning
more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Who's in the Zone? A Qualitative Proof-of-Concept for Improving Remote Access Least-Privilege in ICS-SCADA Environments

Remote access control in many ICS-SCADA environments is of limited effectiveness leading to excessive privilege for staff who have responsibilities bounded by region, site, or device. Inability to implement more restrictive least-privilege access controls may result in unacceptable residual risk from internal and external threats. Security vendors and ICS cybersecurity practitioners have recognized this issue and provide options to address these concerns, such as inline security appliances, network authentication, and ...

Copyright SANS Institute
Author Retains Full Rights



Who's in the Zone?

A Qualitative Proof-of-Concept for Improving Remote Access Least-Privilege in ICS-SCADA Environments

GIAC (GICSP) Gold Certification

Author: Kevin Altman, kaltman@ieee.org

Advisor: Johannes Ulrich

Accepted: NOV 29 2017

Template Version September 2014

Abstract

Remote access control in many ICS-SCADA environments is of limited effectiveness leading to excessive privilege for staff who have responsibilities bounded by region, site, or device. Inability to implement more restrictive least-privilege access controls may result in unacceptable residual risk from internal and external threats. Security vendors and ICS cybersecurity practitioners have recognized this issue and provide options to address these concerns, such as inline security appliances, network authentication, and user-network based access control. Each of these solutions reduces privileges but has tradeoffs. This paper evaluates network-based access control combined with security zones and its benefits for existing ICS-SCADA environments. A Proof-of-Concept (PoC) evaluates a promising option that is not widely known or deployed in ICS-SCADA.

1. Introduction

The National Institute of Standards and Technology (NIST) defines least-privilege as allowing only authorized access necessary to accomplish assigned tasks in accordance with organizational missions and business functions (United States. Joint Task Force Transformation Initiative, 2012). In practice, least-privilege is seldom fully achieved. ICS-CERT cites least-privilege access control as a top-7 Industrial Control System (ICS) weakness in 2014, 2015 and 2016 Assessment Summary Reports (Industrial Control Systems Cyber Emergency Response Team, 2017). Beyond improper implementation, effective least-privilege access control can be problematic in existing (i.e., brownfield) ICS-SCADA environments because of devices that:

- Lack access control. This can occur due to non-existent access control on older PLCs/RTUs ("Overview of Cyber Vulnerabilities | ICS-CERT," n.d.),
- Lack complete access control. This can arise from lack of authentication of significant commands such as modifying set points or system halt (e.g., original insecure variants of ModBus, ICCP, DNP3, and ProfiBus are still used extensively), or
- Lack secure access control. This can occur due to limited-length passwords, hard-coded passwords, or long patch cycles for publicly known vulnerabilities (varies by vendor product or vendor/operator flaw remediation processes).

Because of these realities, an Industrial Control System – Supervisory Control and Data Acquisition (ICS-SCADA) environment's remote access control is often reduced to

who does or does not have access to the ICS-SCADA environment from the enterprise environment. These circumstances can lead to excessive privilege for staff who have responsibilities bounded by region, site, or device type. Further, these realities allow straightforward escalation of privileges for malicious internal or external threats.

Underscoring this, Vávra et al. evaluated 50 vulnerabilities reported by ICS-CERT in the first half of 2015 determining 59% are remotely exploitable, and 84% are exploitable without authentication (Vávra, Hromada, & Jašek, 2015). Given ICS longevity and operational constraints, Vávra et al. findings are still relevant today. Calvo et al. provide further detail on the issues highlighted above and recommends that "Access control must ... [follow] unique identification, role-based authorization and principle of least privilege ..." (Calvo, Etxeberria-Agiriano, Iñigo, & González-Nalda, 2016). Summarizing, the inability to implement effective least-privilege remote access control likely results in unacceptable residual risk to an organization operating ICS.

Network-based access control reduces unacceptable risk due to excessive remote access privilege. This paper describes three options for network-based access control implemented by overlaying Role Based Access Control (RBAC) on security zoning: Option 1 security zone restricted traffic, Option 2 security zone authentication, and Option 3 security zone authenticated user. The first two options are commonly used and briefly summarized for comparison. A lack of knowledge of the third option relative to actual ICS-SCADA architectures overlooks a significant capability to improve remote access least-privilege for brownfield ICS-SCADA sites. This paper will qualitatively evaluate a Proof-of-Concept (PoC) of the third option and its ability to address the issues raised.

2. Background

2.1. ICS-SCADA Reference Architecture Model

The Purdue Enterprise Reference Architecture (PERA) model is an architecture model used to describe enterprises with ICS for clarity on how various systems relate. It was developed in the early 1990s by Theodore J. Williams et al. (Williams, 1991). The PERA model does not represent security zones; rather, it provides a starting point for possible zones based on like systems (technology used and likely process impact). A depiction of the model is below in Figure 1:

Figure 1 Purdue Enterprise Reference Architecture (PERA) Model

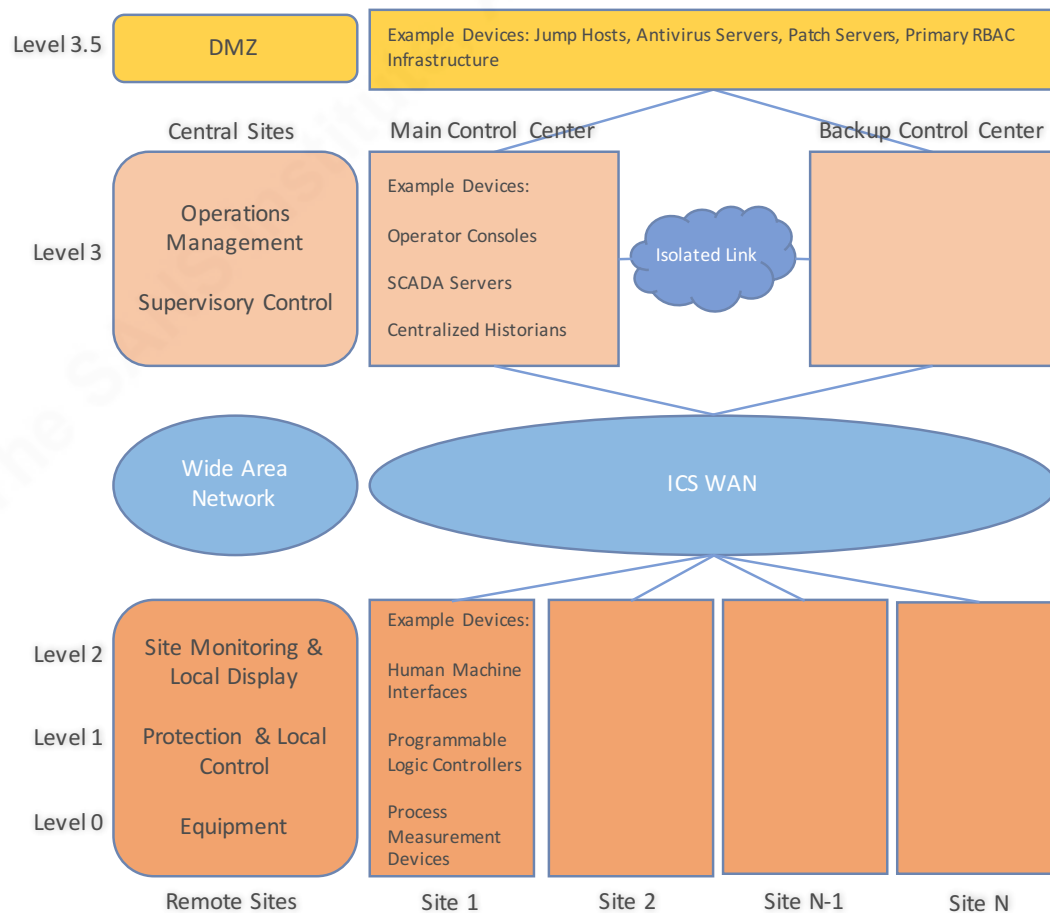


The PERA model originally consisted of five levels, but due to accepted guidance enterprise and ICS, environments are segmented so a Level 3.5 Demilitarized Zone often appears for explicit separation of the ICS environment from the corporate environment.

Multiple organizations have built on, aligned to, or are consistent with the PERA model when defining recommended placement of policy enforcement or security zones

for ICS systems. Most documentation focuses on single site ICS architectures sometimes resulting in misapplication to ICS-SCADA. However, IEC 62443-2-1 Figure A.9 provides a clear ICS-SCADA reference architecture consistent with central control of geographically distributed sites while also aligning with the PERA model. The relevant structure from IEC 62443, with the addition of a DMZ, forms the basis of the PoC representative ICS-SCADA system architecture and is captured in the following diagram:

Figure 2 ICS-SCADA Reference Architecture Aligned to PERA Model



From a communication perspective, implementation of typical ICS-SCADA systems uses a hub-and-spoke architecture (also referred to as star architecture). Levels 3.5/3 form the hub, while the remote sites are the termination of the spokes. Hub-and-spoke enables

least-privilege improvements using security zones as the central and remote sites typically meet most the concepts of zones without having been formally defined as such.

2.2. ICS-SCADA Access Control in Older Systems

The longevity of ICS is well known, leading to many brownfield environments that have security controls well behind state-of-the-art for enterprise environments. A circa 2000 ICS-SCADA¹ deployment, with operational and security updates, possibly looks like this today (NIST, May 2015), (Homeland Security, September 2016), (Obregon, September 2014):

- Level 3.5 DMZ – Centrally Located
 - Limiting access from enterprise to ICS-SCADA environment using Access Control Lists (ACLs)².
 - Containing Jump Host(s) that users outside the ICS-SCADA environment authenticate to before allowing remote access to devices in Levels 3 and below.
 - Possibly containing centrally managed RBAC infrastructure connected to Jump Host(s) and other lower level devices that support RBAC. Note, the RBAC infrastructure may reside in Level 3. The choice is dependent on

¹ Initial deployment or architectural refresh for brownfield sites might date from 1990 – 2010. This period coincided with significant technology change in networking, operating systems, and SCADA applications (Langner, 2012).

² i.e., Rules defining allowable IP address and port number (where appropriate) implemented on routers/firewalls.

implementation of the DMZ for a given enterprise (guidance around placement varies by publication).

- Level 3 – Centrally Located
 - Possibly a separate zone if appropriate ACLs restricting traffic is implemented.
 - Devices with current Operating Systems (OS), possibly utilizing domain accounts (connected to centrally managed RBAC) and some local accounts.
- Levels 2,1,0 – Remotely Located
 - Possibly each remote site is a separate zone if appropriate ACLs restricting traffic is implemented.
 - Devices with varying levels of access control capability, possibly utilizing domain accounts (connected to centrally managed RBAC) or local accounts.
 - Devices with access control shortcomings identified in Introduction.

Generally, the access control summarized above would result in excessive and easily escalated privileges. Fortunately, the structure also provides a basis for implementing reasonable improvements for a brownfield ICS-SCADA environment.

2.3. PoC Constraints, Requirements, and Evaluation Criteria

Least-privilege improvements to brownfield access control based on zoning will likely be implemented for options that do not impact devices in PERA Levels 1 and

below (the process control levels of ICS-SCADA) and as few devices as possible in PERA levels 2 and above. Therefore, the PoC requires the addition of devices necessary for least-privilege improvements to be above PERA Level 1 (Requirement 0).

Analysis of the devices, threats, and consequences in the ICS-SCADA environment determines the appropriate security zones. The likely minimum ICS-SCADA zoning structure would be that which is captured in IEC 62443-2-1 Figure A.9 which has the following zones: central primary site Level 3 zone, central secondary site Level 3 zone, and a single zone at each remote site encapsulating Levels 2, 1, and 0.

A more complex environment would have multiple zones at some sites. Given current threats and organizational factors, this is likely the most appropriate for significant ICS-SCADA environments and is a requirement to be evaluated by the PoC (Requirement 1).

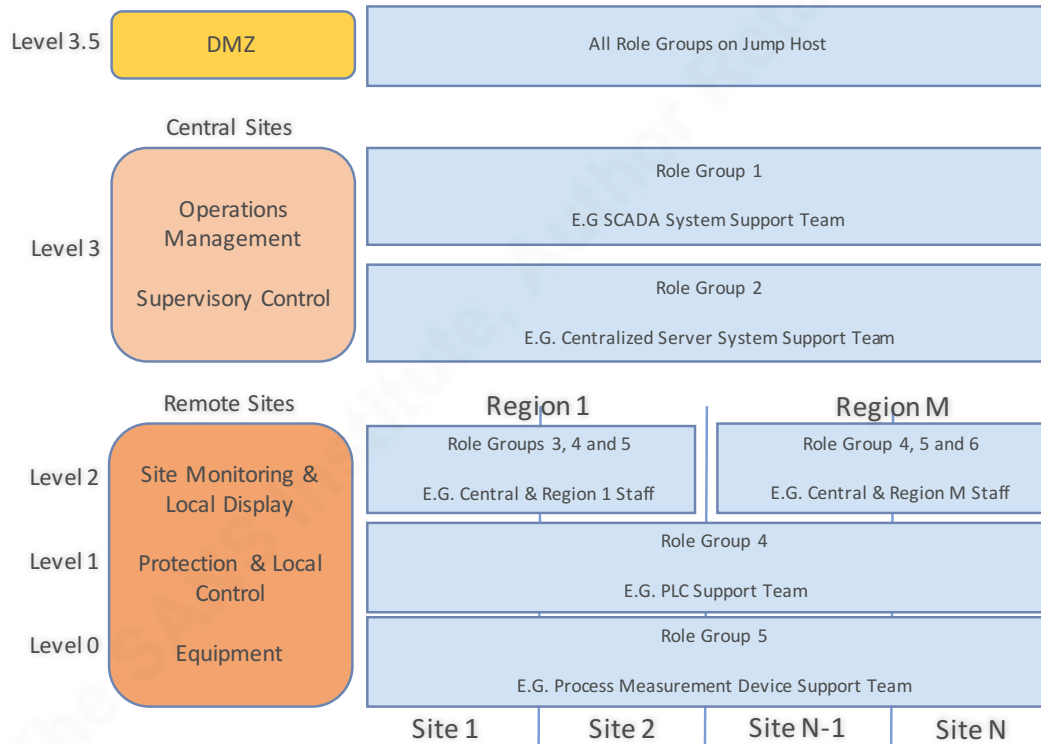
Table 1 PoC Requirements

#	Requirement
R0	Device additions or network modifications must occur above PERA level 1 in the ICS-SCADA environment.
R1	The solution should support multiple zones at each site.
R2	The solution should restrict individual RBAC group zone/device access/visibility for groups with non-overlapping responsibilities defined in Figure 3.
R3	The solution should minimize the number of devices required to implement.
R4	The solution should operate without impairment for remote site ICS WAN characteristics of (1) packet delivery $\geq 99\%$, and (2) round trip latencies ≤ 1 second ³ .
R5	The solution should minimize the amount of SCADA WAN data traffic required to operate.
R6	The solution should operate at a remote site without loss of SCADA WAN link.

³ Verizon's Private IP Satellite Service Level Agreement states (1) Network Packet Delivery $\geq 99\%$, and (2) the monthly average round-trip delay shall be less than 800 milliseconds.

Figure 3 captures the role-based groups to be used in the evaluation of the PoC.

Figure 3 Role Based Groups Requirements Diagram



The PoC role-based groups in Figure 3 (Requirement 2) have been selected to represent potential role-based groups in a reasonably sized ICS-SCADA environment. In summary, these groups evaluate the capability of the solution to implement:

- multiple groups per site,
- separate groups across regions,
- separate Level 2 and 1/0 groups at a field site, and
- separate Level 1/0 group access at a field site using only architecture and system changes above Level 1/0.

The set of groups selected can be extrapolated to more granular access control groups if appropriate such as additional Level 3 roles (such as operators) and Level 2 roles (such as non-control certified staff supporting standard IT infrastructure).

The remaining requirements are based on practicalities: the number of devices required to implement the solution (Requirement 3) and the characteristics of a worst-case ICS WAN (Requirements 4-6).

2.4. Least-Privilege Access Control Options based on Zones

In order of increasing restriction and implementation complexity, the brownfield least-privilege access control options using zoning considered are:

1. Security Zone restricted traffic,
2. Security Zone authentication, and
3. Security Zone authenticated user.

The options require policy enforcement points (PEPs) between the zones. Depending on the requirements for the PEPs, at minimum implement ACLs or maximum authenticate individual users using RBAC infrastructure.

2.4.1. Option 1 Security Zone Restricted Traffic Access Control

For security zone restricted traffic access control, the PEPs between zones are configured to allow only authorized traffic to flow across, such as machine-to-machine traffic and traffic from a single central Jump Host. Practically, many devices on the market can realize this option by ACLs. This option is the least restrictive but is straightforward to implement. It is the least restrictive in that the only ability to limit access is at the Network and Transport layers (by IP address and port number). This

option allows any user with Jump Host privileges visibility of any device in any site or zone that has been determined necessary for business purposes for any of the other users of the Jump Host. Security zone restricted traffic access control is easiest to implement in that the PEPs required to support it are already likely in place, i.e., either routers (questionable effectiveness) or firewalls.

The most significant shortcoming of this option, which the next option addresses, arises because a user with Jump Host access privileges has blanket visibility (and hence, potential access based on issues outlined in the Introduction) to all ICS devices where ACLs allow the traffic. In an ICS-SCADA environment, this results in privilege levels excessive to those necessary for business purposes.

2.4.2. Option 2 Security Zone Authenticated Access Control

For security zone authenticated access control, the PEPs between zones are configured to allow only authorized regular traffic and separately authorized intermittent access. Practically, there are at least two methods of realizing this option: (1) method A (only PEPs) - ACLs and zone authentication on the PEPs, or (2) method B (PEPs & multiple jump hosts) - ACLs and zone authentication by using separate jump hosts per zone. This option is more restrictive than the first but more complex because a zone authentication mechanism is required.

The improvement in restriction occurs by using the ACLs for the regular machine to machine-based traffic and using zone authentication for intermittent human-based traffic. Separating traffic this way reduces user visibility into any zone that is not necessary for business purposes.

The most significant shortcoming of this option, which the next option addresses, arises because a user with zone access privileges has visibility (and hence, potential access) to any device in the zone. In an ICS-SCADA environment, this level of privilege is typically beyond what is necessary for business purposes.

2.4.3. Option 3 Security Zone User Authenticated Access Control

For security zone user authenticated access control, the PEPs between zones are configured to allow only authorized regular traffic and separately authorized access by user group. Practically, this is realized by PEPs that direct traffic into the zone based on user group. This option is the most restrictive of the three outlined in this paper but requires advanced PEPs.

The improvement in restriction occurs by using the ACLs for regular machine-to-machine based traffic and user authentication for human-based traffic. This option ensures users external to the zone have visibility of only devices necessary for business purposes.

The most significant shortcoming of this option, which is not directly addressable by the PoC zoning model, arises because a user who has authenticated onto a device inside the zone then has visibility (and hence, potential access) to any other device in the zone. This shortcoming can be addressed by (1) further division with each additional zone likely adding cost and complexity, or by (2) access control on the individual devices which may be problematic given the issues outlined in the Introduction.

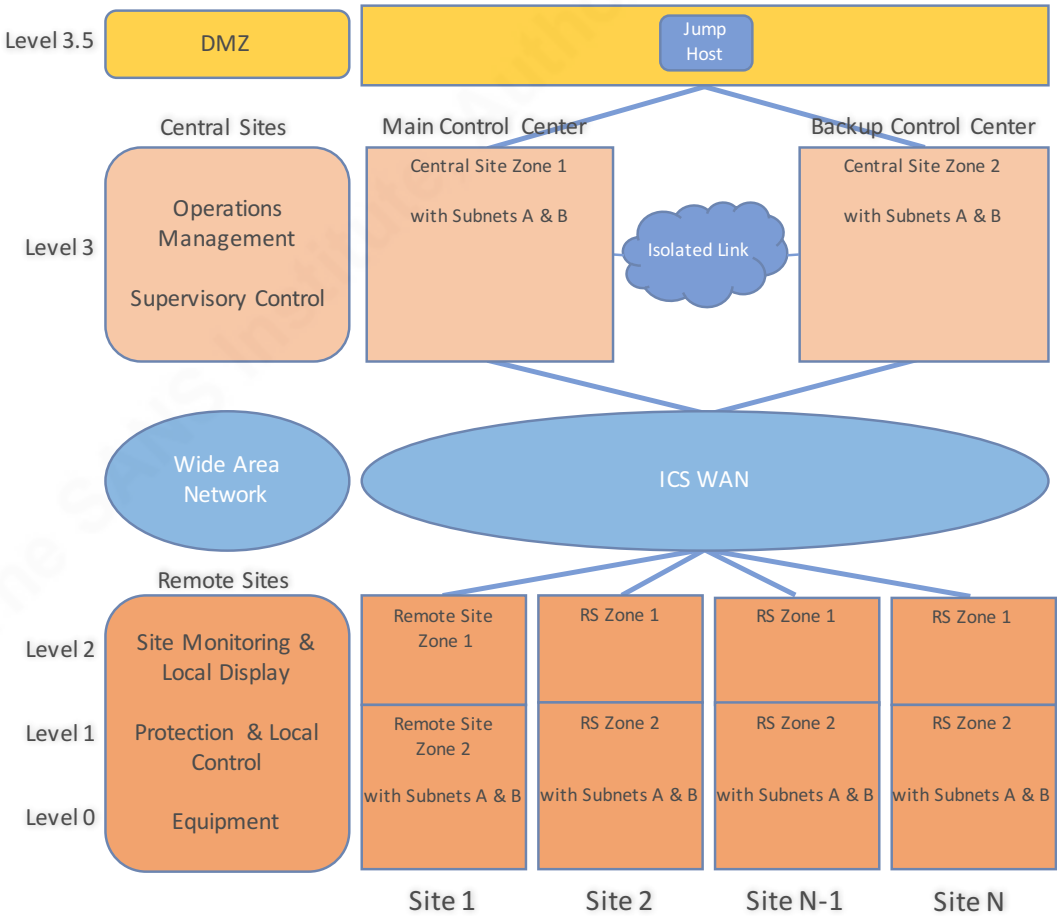
2.4.4. General Comparison of Options

IEC 62443 Figure A.9 (simplified re-creation in Figure 2) represents each site (all central and remote) as separate zones. While not explicitly outlining why this is so, risk

analysis and practical realities for ICS-SCADA environments of reasonable complexity and process safety failure consequence justify at least this level of zoning.

To meet the PoC requirements regarding least-privilege for the groups outlined in Figure 3 requires further zoning. Figure 4 captures the zoning architecture necessary.

Figure 4 Zoning & System Architecture based on Requirements



Based on general characteristics of the options and the zoning architecture in Figure 4, the following Table 2 captures a preliminary analysis against the requirements.

Table 2 Comparison of Security Zoning Access Control Options

Requirement	Option 1 Restricted Traffic (Least Restrictive)	Option 2 Zone Authenticated	Option 3 User Authenticated (Most Restrictive)
R0 PERA Level Impact	Met by design.	Met by design.	Met by design.
R1 Multiple Site Zones	Pass. No limitation on multiple zones at a site.	Pass. No limitation on multiple zones at a site.	Pass. No limitations on multiple zones at a site.
R2 RBAC Least-Privilege	Fail. Note, dividing network below level 1 with this option provides no further benefit to achieve R3.	Method A – Fail. Dividing network below level 1 is required to achieve R3. Method B – Pass.	PoC will evaluate.
R3a Devices Required - Jump Hosts	1	Method A – 1, or Method B – 1 per zone minimum plus 1 per restricted zone subnet.	1 central, 1 per remote site.
R3b Devices Required - Policy Enforcement Points	1 per zone, and ACL capable.	1 per zone, ACL capable, and Zone authentication capable (method A).	1 per zone, ACL capable, and User authentication capable.
R3c Devices Required - RBAC Infrastructure	Not required.	Optional. May use RBAC to support transparent authentication.	Required.
R4 ICS WAN Performance	Pass. No data transfer loss or latency issues.	Pass. No data transfer loss or latency issues.	PoC will evaluate.
R5 ICS WAN Traffic	Requires 0 kilobits/sec of additional traffic.	RBAC will require similar traffic as User Authentication Option.	PoC will evaluate.
R6 ICS WAN Loss	No impact.	Requires each remote site to have local RBAC repository.	Requires each remote site to have local RBAC repository.

3. Option 3 Security Zone User Authentication PoC Evaluation

Figure 4 above defines the ICS-SCADA architecture while Table 3 below captures the systems aligned to the architecture required to evaluate security zone user authentication based on Palo Alto Networks' UserID.

Table 3 Option 3 PoC System Summary

Enterprise Zone
<ul style="list-style-type: none"> Enterprise System – Commercial OS with Microsoft Remote Desktop client.
Level 3.5 DMZ
<ul style="list-style-type: none"> PEP – Palo Alto Networks PA-220 Unit A controlling access in/out of zone, DMZ Jump Host – Microsoft Server 2012 R2 OS system with Remote Desktop enabled, and Palo Alto Networks Terminal Services Agent installed, and Main Active Directory – Microsoft Server 2012 R2 running Active Directory for PEPs, Jump Hosts, and appropriate systems.
Level 3 Zone
<ul style="list-style-type: none"> PEP – Palo Alto Networks PA-220 Unit A controlling access in/out of zone, L3 System – Microsoft Windows 7 Professional OS system representing a generic central management system, and Poller – Microsoft Server 2012 R2 OS system representing a SCADA system for transmitting/receiving SCADA traffic to/from the remote site Level 1 devices.
WAN
<ul style="list-style-type: none"> ICS WAN - Microsoft Windows 7 Professional OS system running SoftPerfect's Connection Emulator Pro in bridge mode.

<p>Site 1 Level 2 Zone</p> <ul style="list-style-type: none">○ PEP – Palo Alto Networks PA-220 Unit B controlling access in/out of zone,○ Site Jump Host – Microsoft Server 2012 R2 OS system with Remote Desktop enabled, and Palo Alto Networks Terminal Services Agent installed,○ Site Read-Only Active Directory – Microsoft Server 2012 R2 running Active Directory for PEPs, Jump Hosts, and appropriate systems, and○ L2 System – represents possible level 2 devices found at remote sites such as Data Historians or monitoring Human Machine Interfaces (HMIs).
<p>Site 1 Levels 1/0 Zone</p> <ul style="list-style-type: none">○ PEP – Palo Alto Networks PA-220 Unit B controlling access in/out of zone (same physical hardware as the Level 2 PEP),○ Type A Device - Embedded device such as a PLC, and○ Type B Device - Generic Process Measurement Device.

In a full implementation, more infrastructure systems than those listed would be required to meet the high availability needs of ICS-SCADA (e.g., redundant PA-220s and Active Directory servers, etc.); however, for the PoC the selected systems were sufficient to evaluate the impact of UserID on access privileges.

3.1. Requirement 2 RBAC Least-Privilege PoC Evaluation

For ICS-SCADA environments having devices with weak access controls, separate zones for separate Role Groups provide the most consistent guarantee of maintaining remote access least-privilege. However, sub-zoning is typically not practical for most brownfield sites at Levels 1 and below (hence Requirement R0). Furthermore, many control systems have timing critical communication in Levels 1 and below which may also restrict the applicability of further sub-zoning in greenfield (i.e., new) sites. Requirement 2 evaluates the PoC's capability to restrict access under these constraints.

To understand how access would be controlled in an actual ICS system, the following figure, Figure 5, represents the defined PoC user group traffic and some inter-zone traffic expected in a typical ICS-SCADA environment. For reference, the diagram also includes some machine-to-machine (e.g., traffic restricted by only ACLs) traffic and Site N traffic.

Figure 5 Representative Interzone Communication

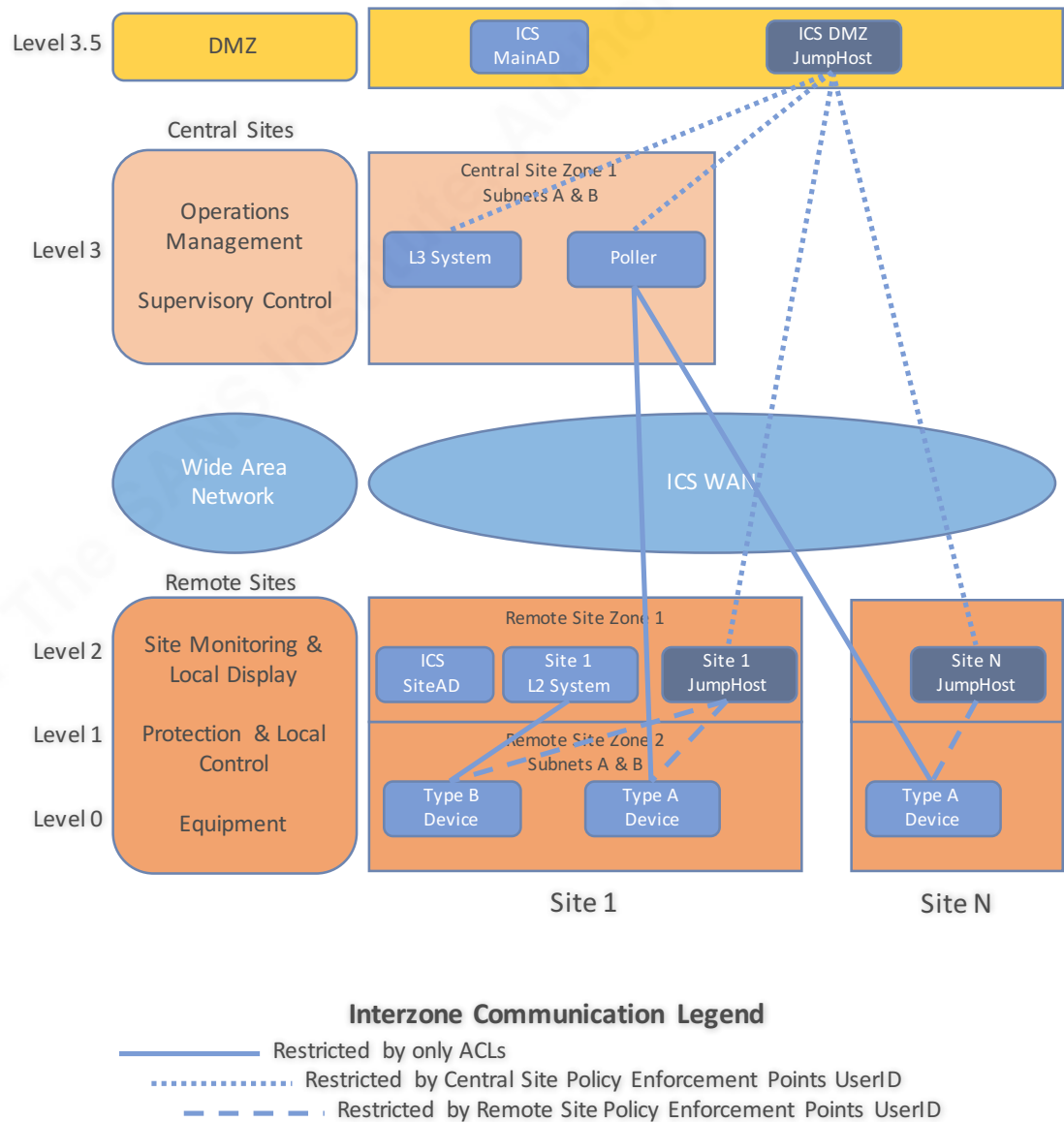


Table 4 below assesses that the PoC achieves Requirement 2 for each of the defined role groups.

Table 4 Assessment of Requirement 2

Group	Requirement Assessment The solution should restrict individual RBAC group zone/device access/visibility for groups with non-overlapping responsibilities defined in Figure 3.
Role Group 1	Pass. Testing confirmed that when logged onto the ICS DMZ Jump Host, Group 1 does not have visibility (and hence direct access) of systems in any of the other defined zones or subnets. This group's direct access was limited to Central Zone 1 Subnet A.
Role Group 2	Pass. Testing confirmed that when logged onto the ICS DMZ Jump Host Group 2 does not have visibility (and hence, direct access) of systems in any of the other defined zones or subnets. This group's direct access was limited to Central Zone 1 Subnet B.
Role Group 3	Pass. Testing confirmed that when logged onto the ICS DMZ or Site 1 Jump Hosts Group 3 does not have visibility (and hence, direct access) of systems in any of the other defined zones. This group's direct access was limited to Site 1's Zone 1.
Role Group 4	Pass. Testing confirmed that when logged onto the ICS DMZ or Site 1 Jump Hosts Group 4 does not have visibility (and hence, direct access) of systems in any of the other defined zones or subnets. This group's direct access was limited to Site 1's Zone 1 and Zone 2 Subnet A.
Role Group 5	Pass. Testing confirmed that when logged onto the ICS DMZ or Site 1 Jump Hosts Group 5 does not have visibility (and hence, direct access) of systems in any of the other defined zones or subnets. This group's direct access was limited to Site 1's Zone 1 and Zone 2 Subnet B.
Role Group 6	Pass. Testing confirmed that when logged onto the ICS DMZ Jump Host, Group 6 does not have visibility (and hence, direct access) of systems in any of the other defined zones.

After granting access to a zone or device, additional least-privilege restrictions are reliant on the access controls of the other devices inside the zone as there is no expectation of intra-zone communication restrictions by the network (though this can be accomplished if the network devices support integration with the PA-220s).

3.2. Requirement 3 Devices Required PoC Evaluation

Direct comparison of devices required for implementation is only possible for Option 2 Method B given that this solution can technically replicate the same level of access control implemented in the PoC for the defined zones. As highlighted in Table 5 significantly more Jump Hosts are required.

Table 5 Assessment of Requirement 3

Parameter	Requirement Assessment The solution should minimize the number of devices required to implement.
Central Policy Enforcement Points	Pass. Implementation of UserID to reduce least-privilege does not require additional policy enforcement points beyond those used to create individual zones.
Site Policy Enforcement Points	Pass. Implementation of UserID to reduce least-privilege does not require additional policy enforcement points beyond those used to create individual zones.
Jump Hosts	Pass. UserID minimizes central Jump Hosts to one centrally and one at each remote site. To achieve the same level of least-privilege, Option 2 Method B requires: <ul style="list-style-type: none"> • 2 + M Central Jump Hosts (one for each of Groups 1 & 2, and each Region), and • 3 x N for Site Jump Hosts (one for each of groups 3, 4, 5 and 6 with different privileges onsite).
Active Directory	Pass. An instance of Read-Only Active Directory is required onsite to support the availability requirements of user groups for Microsoft Windows systems which UserID can then leverage.

3.3. Requirement 4 ICS WAN Performance PoC Evaluation

SoftPerfect's Connection Emulator Pro was utilized to emulate the performance of a "worst case" WAN link with the settings defined in Table 6.

Table 6 ICS WAN Settings

Parameter	Setting
Transfer Rate	256 kbps each direction

Parameter	Setting
Latency	500 msec each direction
Packet Loss	1%

The following screen capture of the Emulator provides a high-level overview of its capability (Figure 6) to restrict data rate, add latency, and manipulate individual packets. The Emulator can also monitor, at a high level, upstream and downstream traffic.

Figure 6 SoftPerfect Connection WAN Emulator

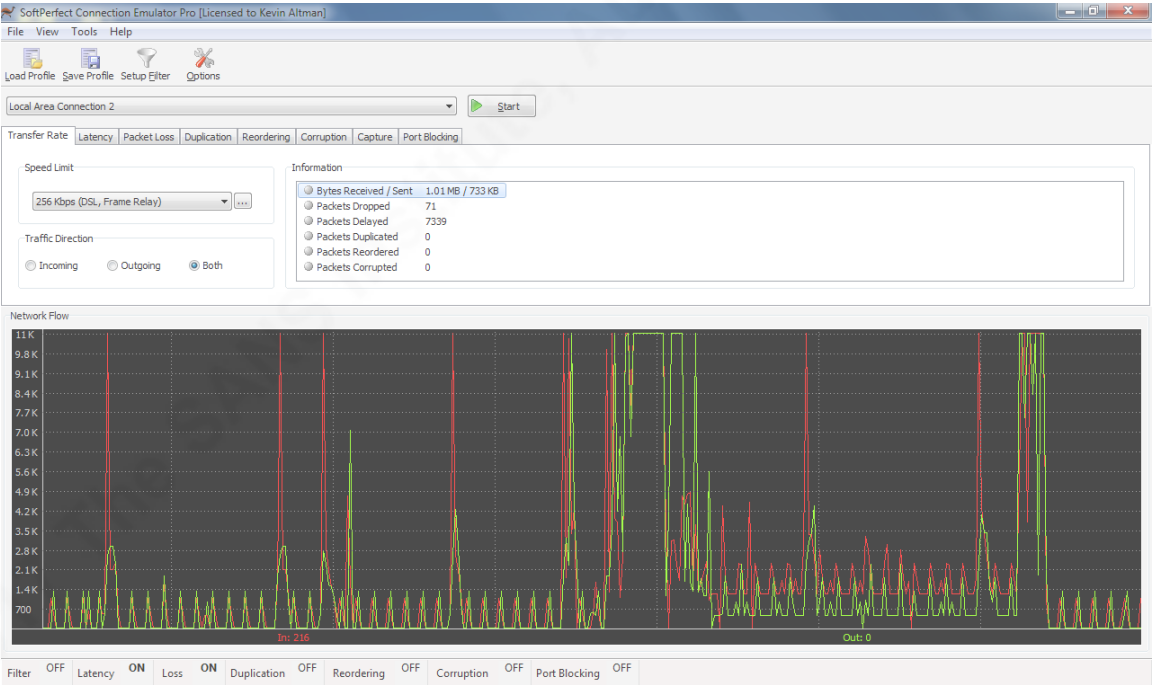


Table 7 Assessment of Requirement 4

Parameter	Requirement Assessment
	The solution should operate without impairment with remote site SCADA WAN characteristics of (1) packet delivery $\geq 99\%$, and (2) round trip latencies ≤ 1 second.
Packet Loss = 1%	Pass. The PoC did not exhibit any discernable issues.
Latency = 1 second roundtrip	Pass. The PoC (User ID or RBAC using Active Directory) did not exhibit any discernable issues. However, as expected, the latency impacted the performance of Remote Desktop. Significant time-lag required adjustment of the user interactions with the remote operating system and applications.

3.4. Requirement 5 ICS WAN Traffic PoC Evaluation

Wireshark was utilized to evaluate the data requirements on the traffic over the ICS WAN between the Central and Remote Site 1.

Table 8 ICS WAN Traffic Required for UserID

Traffic Type	Direction	Data Rate (average)
Palo Alto Networks Terminal Service Agent	JumpHost → Site PA-220	225 – 500 bits/sec.
	Site PA-220 → JumpHost	250 – 500 bits/sec.
Active Directory Services	MainAD → ROADC	200 – 300 bits/sec.
	ROADC → MainAD	600 – 1000 bits/sec.

As the table above shows, traffic fluctuated slightly over the course of the period monitored (several hours). The following three figures provide several views of the various traffic patterns to support UserID at a remote site.

The legend for each figure is as follows:




-  Data traffic between the Site 1 PA-220 and the ICS DMZ Jump Host (hosting the Palo Alto Networks Terminal Server Agent).
-  Data traffic between the domain controllers MainAD (in ICS DMZ) and ROADC (in Site 1).
-  Data traffic (on the last diagram) between the ICS DMZ and Site 1 Jump Hosts during a Microsoft RDP session.

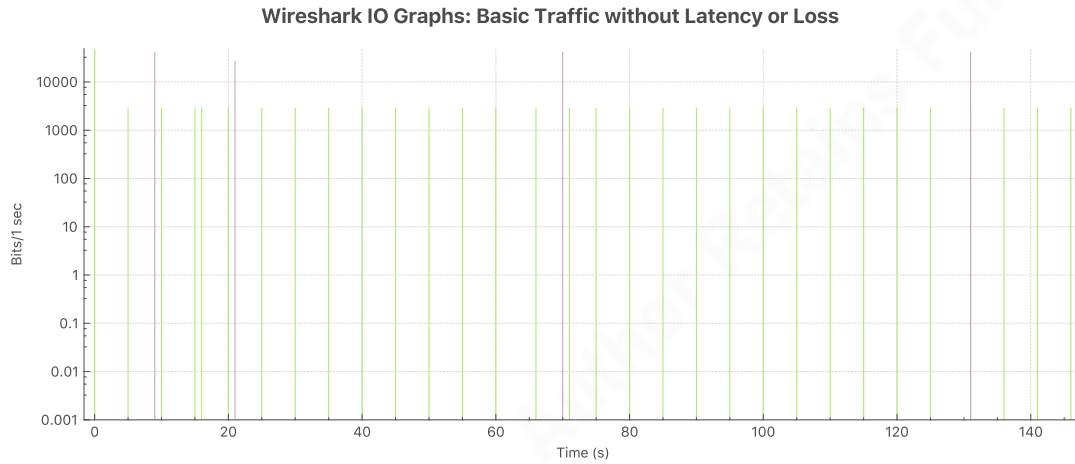
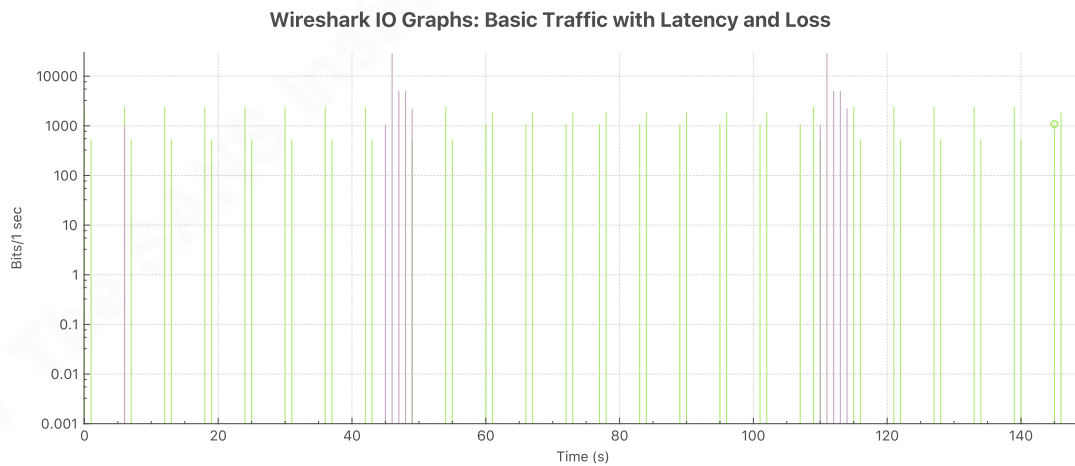
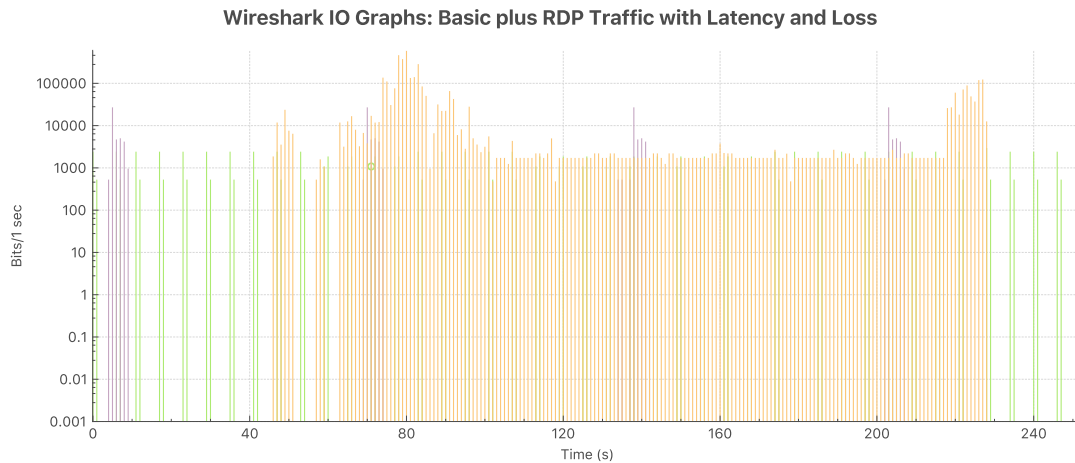
Figure 7 ICS WAN Traffic (UserID and Domain Controller) without Latency or Loss*Figure 8 ICS WAN Traffic (UserID and Domain Controller) with Latency and Loss**Figure 9 ICS WAN Traffic (UserID, Domain Controller, and RDP) with Latency and Loss*

Table 9 Assessment of Requirement 5

Parameter	Requirement Assessment The solution should minimize the amount of SCADA WAN data traffic required to operate.
Palo Alto Networks Terminal Services Agent Traffic	Pass. Reductions in data traffic for the Terminal Services Agent is not possible as the 5 second polling period is fixed based on current feedback from Palo Alto Networks. Fortunately, the measured traffic data rate is low.
Active Directory Traffic	Pass. The PoC Active Directory traffic was not analyzed for reduction as the data rate is considered sufficiently low. In any case, a Read-Only Active Directory controller is required at each remote site to support high availability of domain accounts for ICS-SCADA operational reasons.

3.5. Requirement 6 ICS WAN Loss PoC Evaluation

Utilization of a Read-Only Active Directory controller at each remote site provides the capability for UserID to function when the ICS WAN link is down.

Table 10 Assessment of Requirement 6

Parameter	Requirement Assessment The solution should operate at a remote site without loss of SCADA WAN link.
ICS WAN link severed	Pass. UserID remained functional in restricting access into Zone 2, thereby managing privileges as designed for subnets A & B when users logged onto the Site Jump Host.

4. Conclusion

Security zone user authenticated access control implemented with Palo Alto Networks' UserID met all PoC requirements outlined in Table 1. Security zone user authentication supports the implementation of remote access least-privilege across regions, sites, and PERA levels. Further, this option required the least ICS architecture modification of the two options meeting the requirements.

Central and Remote Site Jump Hosts utilizing UserID provide independent incremental improvement of remote access least-privilege. The Central Jump Host provides group specific restricted access into the central zones and remote zones. In some ICS architectures, this may be sufficient. The hub-and-spoke architecture of typical ICS-SCADA environments enables significant improvement in remote access least-privilege by adjustments of the centralized controls. Further, modification of central versus remote site controls is typically easier to accomplish in an existing (i.e., brownfield) environment.

Remote Site Jump Host provided group specific restricted access between site zones once inside a remote site. In some circumstances, implementation could consider other means such as host/application partitioning in Zone 1 combined with centralized UserID to achieve an almost similar reduction in privilege without the need for a local Jump Host.

If Jump Host(s) are already utilized to control remote access, the addition of UserID based on zones is transparent to the users which is a significant factor in a successful implementation given the diversity of users in a typical ICS-SCADA environment.

The PoC also evaluated targeting of remote access to subnets and specific devices inside the zone. Targeting was accomplished directly using the capabilities of the PA-220s and is a potentially powerful build on pure zone based access control for a remote site. The first benefit is the ability to force remote access to specific systems in a zone that is easy to patch and maintain in a hardened state. The second is to provide a level of remote access control to devices inside PERA Levels 1/0 that do not natively have access control (e.g., PLCs/RTUs running insecure ICS protocols or lacking in access control).

Palo Alto Networks (and likely competitor) systems offer capability to manage access directly which may remove the need for a Jump Host while still meeting the requirements. This was not investigated but offers an interesting possibility to reduce the number of systems required in an implementation. A further benefit is to ensure an important security function is contained in a security device. Evaluation of this capability could be considered for an extension of this paper.

References

- Calvo, I., Etxeberria-Agiriano, I., Iñigo, M. A., & González-Nalda, P. (2016). *Key Vulnerabilities of Industrial Automation and Control Systems and Actions to Prevent Cyber-Attacks*. International Journal of Online Engineering (iJOE), 12(1), 9. doi:10.3991/ijoe.v12i1.4888
- Homeland Security (2016). *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.
- Industrial Control Systems Cyber Emergency Response Team. (2017). *ICS-CERT Annual Assessment Report*. Retrieved from NCCIC website: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf
- International Electrotechnical Commission. IEC Technical Committee 65. (2009). *Industrial communication networks--network and system security: Part 1-1*. Geneva: International Electrotechnical Commission.
- International Electrotechnical Commission. IEC Technical Committee 65. (2010). *Industrial communication networks--network and system security: Part 2-1*. Geneva: International Electrotechnical Commission.
- Langner, R. (2012). *Robust control system networks: How to achieve reliable control after Stuxnet*. New York: Momentum Press.
- Obregon, L. (2015). *Secure Architecture for Industrial Control Systems*. SANS Institute.
- Overview of Cyber Vulnerabilities | ICS-CERT. (n.d.). Retrieved from <https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities#under>

Palo Alto Networks. (2015). *SCADA and Industrial Control Systems Industry Solution Brief*. Retrieved from [https://origin-](https://origin-www.paloaltonetworks.com/resources/techbriefs/scada-ics-solution-brief)

[www.paloaltonetworks.com/resources/techbriefs/scada-ics-solution-brief](https://origin-www.paloaltonetworks.com/resources/techbriefs/scada-ics-solution-brief)

Palo Alto Networks. (2016). *User-ID Tech Brief*. Retrieved from

<https://www.paloaltonetworks.com/resources/techbriefs/user-id-tech-brief>

Palo Alto Networks. (2017). *Ignite Workshop: Hands-on Workshop Industrial Cybersecurity Lab Guide*.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. (2015). *Guide to and Industrial Control Systems Security (ICS) Security*. NIST special publication 800-82.

United States. Joint Task Force Transformation Initiative. (2012). *Security and privacy controls for federal information systems and organizations*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

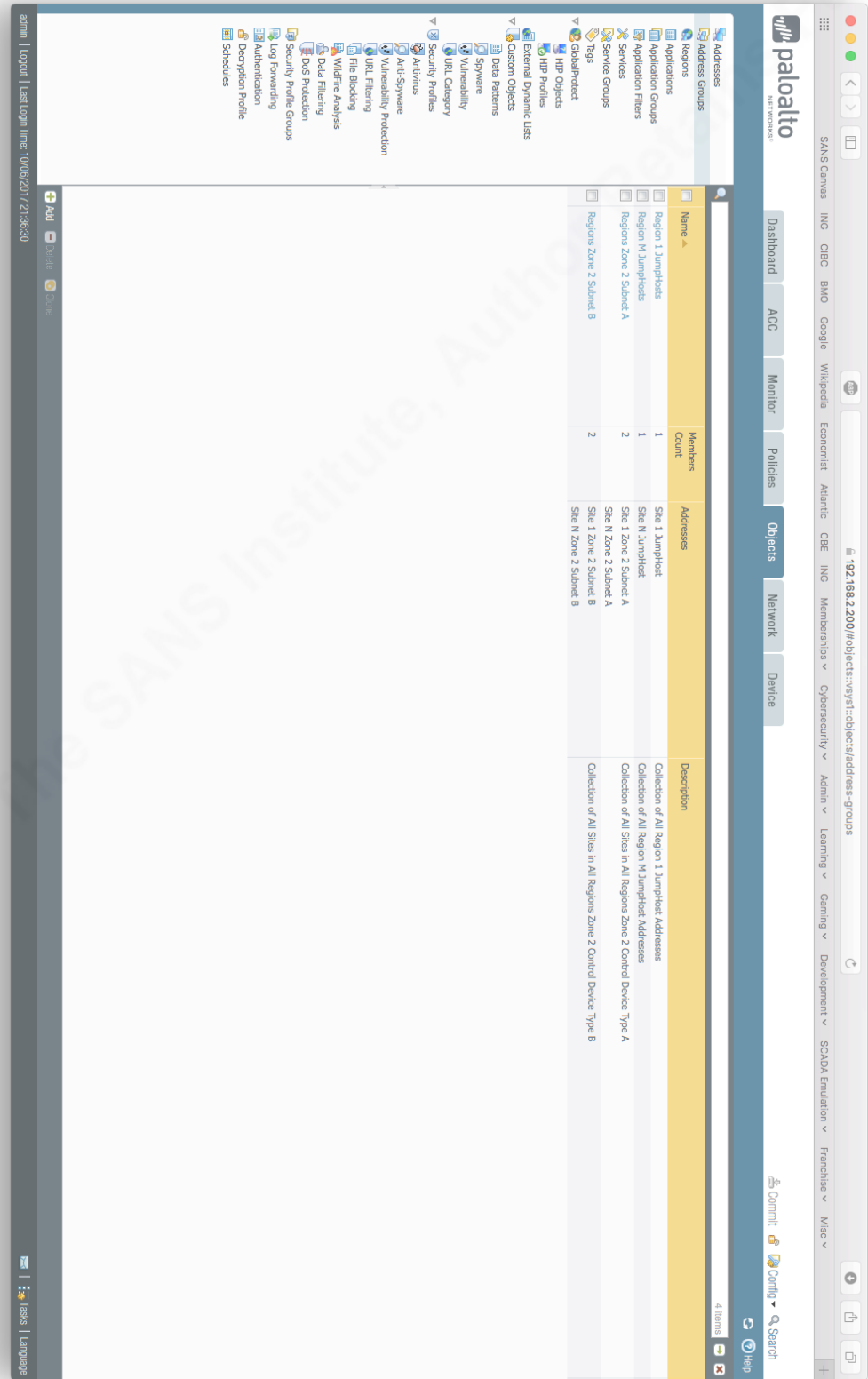
Vávra, J., Hromada, M., & Jašek, R. (2015). *Specification of the Current State Vulnerabilities Related to Industrial Control Systems*. International Journal of Online Engineering (iJOE), 11(5), 64. doi:10.3991/ijoe.v11i5.4981

Williams, T. J. (1991). *A reference model for computer integrated manufacturing (CIM): A description from the viewpoint of industrial automation : prepared by CIM Reference Model Committee International Purdue Workshop on Industrial Computer Systems*. North Carolina: Instrument Society of America.

Central PA-220 – Policies: Security



Central PA-220 – Objects: Address Groups



SANS Carnies ING CIBC BMO Google Wikipedia Economist Atlantic CBE ING Memberships v Cybersecurity v Admin v Learning v Gaming v Development v SCADA Emulation v Franchisees v Misc v

192.168.2.200/#objects:/sys::objects:addresses

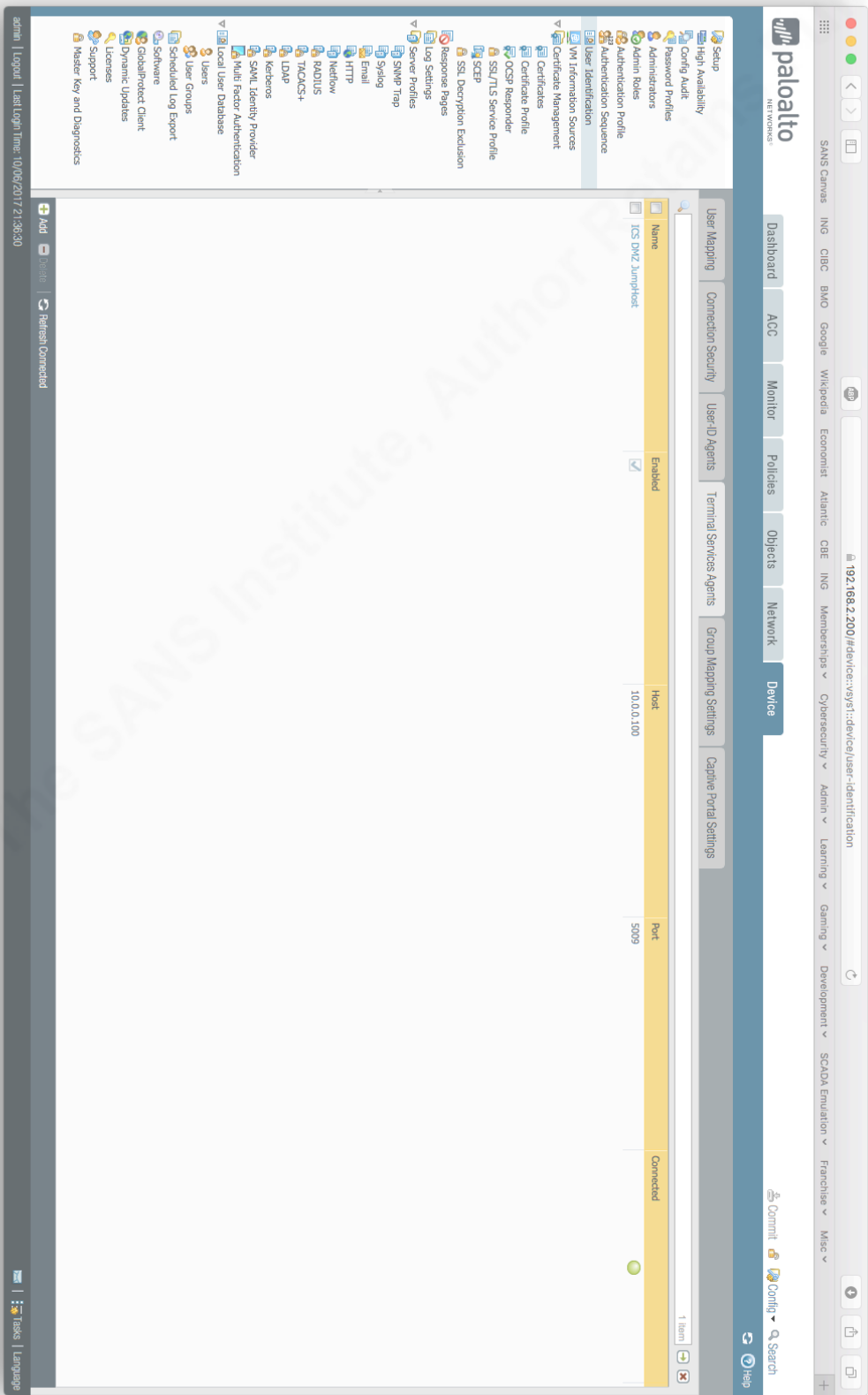
17 items

Dashboard ACC Monitor Policies Objects Network Device

Search

Name	Type	Address	Description
Enterprise JumpHost	IP Netmask	192.168.1.100	Enterprise Address of JumpHost in ICS DMZ
ICS Central Zone	IP Netmask	10.0.1.1/24	ICS Central Zone Subnet
ICS CentralZ Puller	IP Netmask	10.0.1.150	SCADA Puller located in ICS Central Zone Subnet B communicating with Type A Device at each remote site.
ICS CentralZ Subnet A	IP Netmask	10.0.1.1/25	ICS Central Zone subnet for all devices of Type A
ICS CentralZ Subnet B	IP Netmask	10.0.1.129/25	ICS Central Zone Subnet for all devices of Type B
ICS DMZ	IP Netmask	10.0.0.1/24	DMZ Subnet between Enterprise and ICS
ICS DMZ JumpHost	IP Netmask	10.0.0.100	DMZ JumpHost IP Address
ICS WAN Control	IP Netmask	10.0.3.1	IP Address of Central side of WAN link
Hemaid	IP Netmask	10.0.0.200	Main Active Directory Server for ICS Address
Site 1 JumpHost	IP Netmask	10.0.4.100	Site JumpHost IP Address
Site 1 RPODC	IP Netmask	10.0.4.50	Remote Site 1 Read Only Active Directory Controller
Site 1 Zone 2 Subnet A	IP Netmask	10.0.4.129/26	Remote Site 1 Zone 2 Subnet for Control Devices Type A
Site 1 Zone 2 Subnet B	IP Netmask	10.0.4.129/26	Remote Site 1 Zone 2 Subnet for Control Devices Type B
Site N RPODC	IP Netmask	10.0.50.50	Remote Site 1 Read Only Active Directory Controller
Site N JumpHost	IP Netmask	10.0.50.100	Site JumpHost IP Address
Site N Zone 2 Subnet A	IP Netmask	10.50.129/26	Remote Site N Zone 2 Subnet for Control Devices Type A
Site N Zone 2 Subnet B	IP Netmask	10.50.192/26	Remote Site N Zone 2 Subnet for Control Devices Type B

Central PA-220 – Device: User Identification



Central PA-220 – Network: Interfaces

Interfaces

Virtual Wires

Virtual Routers

IPsec Tunnels

DHCP

DNS Proxy

GlobalProtect

Portals

Gateways

MDM

Device Block List

Clientless Apps

Clientless App Groups

QoS

Network Profiles

GlobalProtect IPsec Crypto

IPsec Gateways

IPsec Crypto

Monitor

Interface Mgmt

Zone Protection

QoS Profile

LDP Profile

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Ethernet

VLAN

Loopback

Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Enterprise Jumphost	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet/1	Layer3	Mgt Profile				default	Untagged	none	Enterprise		Access to Private Levels 4, 5 and Internet
ethernet/2	Layer2			none		none	Untagged	ICS DMZ	ICS DMZ.L2		
ethernet/3	Layer2			none		none	Untagged	ICS DMZ	ICS DMZ.L2		
ethernet/4	Layer2			none		none	Untagged	ICS DMZ	ICS DMZ.L2		
ethernet/5	Layer2			none		none	Untagged	ICS CentralZ	ICS CentralZ.L2		
ethernet/6	Layer2			none		none	Untagged	ICS CentralZ	ICS CentralZ.L2		
ethernet/7	Layer2			none		none	Untagged	ICS CentralZ	ICS CentralZ.L2		
ethernet/8	Layer3	Mgt Profile			ICS WAN Central	default	Untagged	none	ICS WAN		

8 Items

Help

Log out | Last login time: 10/09/2017 21:36:30

Add Sub-Interface

Add Aggregate Group

Devices

Tasks

Language

Remote PA-220 – Policies: Security

Kevin Altman, kaltman@ieee.org

Remote PA-220 – Objects: Addresses

paloalto

NETWORKS

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Addresses

Regions

Applications

Application Groups

Application Filters

Services

Service Groups

Tags

GlobalProtect

HTTP Objects

HTTP Profiles

External Dynamic Lists

Custom Objects

Data Patterns

Spyware

Vulnerability

URL Category

Security Profiles

Antivirus

Vulnerability Protection

URL Filtering

File Blocking

Wireless Analysis

Data Filtering

IPS Protection

Security Profile Groups

Log Forwarding

Authentication

Decryption Profile

Schedules

13 Items

Name	Type	Address	Description
ICS Control/Smart B	IP Network	10.0.1.1/24	Contains SCADA based systems that communicate with remote sites
ICS DMZ JumpHost	IP Network	10.0.0.100	Remote Site 1 IP Address viewed from WAN
ICS WAN Site 1	IP Network	10.0.4.1	Main Active Directory Server Address located in ICS DMZ
MainAD	IP Network	10.0.0.200	Remote Site 1 JumpHost IP Address
Site 1 JumpHost	IP Network	10.0.4.100	Remote Site 1 Level 2 System IP Address
Site 1 L2 System	IP Network	10.0.4.125	Read Only Active Directory Controller
Site 1 RPO/DC	IP Network	10.0.4.50	Contains Site Monitoring, Local Display and Other I/O Services.
Zone 1	IP Network	10.0.4.2/25	Contains control system devices.
Zone 2	IP Network	10.0.4.129/25	Contains devices managed by a single group. For example PLCs.
Zone 2 Subnet A	IP Network	10.0.4.129/26	Contains devices managed by a single group. For example Process Measurement Devices.
Zone 2 Subnet B	IP Network	10.0.4.192/26	Representative I/I Device
Zone 2 Type A Device	IP Network	10.0.4.150	
Zone 2 Type B Device	IP Network	10.0.4.250	Representative I/I Device

Commit

Config

Search

Help

admin | Logout | LastLogin Time: 10/04/2017 09:55:43

13 Items

Tests | Language

Remote PA-220 – Network: Interfaces

pal Alto

NETWORKS

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Commit

Config

Search

Help

192.168.2.201/network:vsys1:network/interfaces

Ethernet

VLAN

Loopback

Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet/1	Layer3	Mgt Profile	Up	ICS WAN Site 1	default	Untagged	none	WAN		
ethernet/2	Layer2		Up	none	none	Untagged	ZONE 1	ZONE 1.12		
ethernet/3	Layer2		Up	none	none	Untagged	ZONE 1	ZONE 1.12		
ethernet/4	Layer2		Up	none	none	Untagged	ZONE 1	ZONE 1.12		
ethernet/5	Layer2		Up	none	none	Untagged	ZONE 2	ZONE 2.12		
ethernet/6	Layer2		Up	none	none	Untagged	ZONE 2	ZONE 2.12		
ethernet/7	Layer2		Up	none	none	Untagged	ZONE 2	ZONE 2.12		
ethernet/8	Layer2		Up	none	none	Untagged	ZONE 2	ZONE 2.12		

8 items

Interfaces

VLANs

Virtual Wires

Virtual Routers

IPSec Tunnels

DHCP

DNS Proxy

Globalprotect

Portals

Gateways

NM

Device Block List

Clientless Apps

Clientless App Groups

QoS

LLDP

Network Profiles

Globalprotect IPSec Crypto

IKE Gateways

IPSec Crypto

IKE Crypto

Monitor

Interface Mgmt

Zone Protection

QoS Profile

LLDP Profile

admin | Logout

Last Login Time: 10/04/2017 09:54:43

root@Switch001

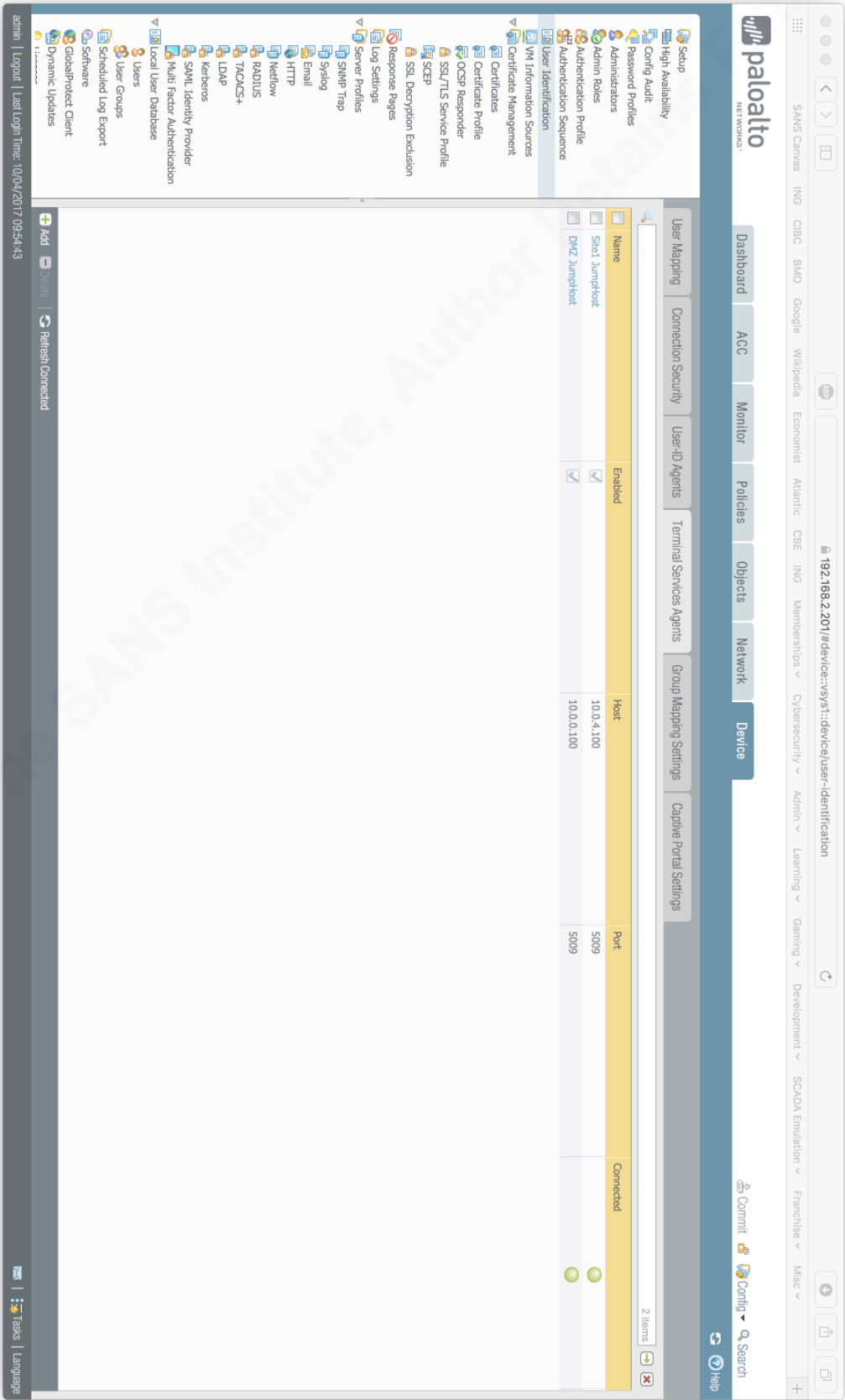
Add Aggregate Group

Devices

Tasks

Language

Remote PA-220 – Device: User Identification



Appendix C Main Active Directory Configuration





Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS SEC455: SIEM Design Beta One 2018	Arlington, VAUS	Feb 12, 2018 - Feb 13, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VAUS	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
ICS Security Summit & Training 2018	Orlando, FLUS	Mar 19, 2018 - Mar 26, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
SEC599: Defeat Advanced Adversaries	OnlineCAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced